Laboratorio Wireshark: DNS

Versione 2.1 italiano
© 2007 J.F. Kurose, K. W. Ross. All rights reserved.
Traduzione italiana di G. Amato, Ottavio M. D'Antona.
Modifiche e adattamenti per il CLEII di G. Amato.

Come descritto nella Sezione 2.5 del libro di testo, il Domain Name System (DNS) traduce nomi di host in indirizzi IP, ricoprendo un ruolo cruciale nella infrastruttura di Internet. In questa lezione daremo uno sguardo più approfondito al lato client del DNS. Ricordate che il ruolo del client nel DNS è piuttosto semplice – un client invia una richiesta al suo server DNS locale, e riceve una risposta. Come mostrato in Figura 2.21 e 2.22 del libro di testo, molte cose avvengono "dietro le quinte", invisibili ai client DNS, quando i server DNS gerarchici comunicano tra di loro ricorsivamente o iterativamente per rispondere alla query. Dal punto di vista del client, però, il protocollo è piuttosto semplice – una query viene inviata al server DNS locale e una risposta viene ricevuta in conseguenza di ciò. Prima di iniziare il laboratorio, fareste probabilmente meglio a rivedere il funzionamento del DNS leggendo la Sezione 2.5 del libro. In particolare, potreste voler rivedere il materiale sui server DNS locali, cache DNS, record e messaggi DNS, e il campo TYPE dei record DNS.

Nslookup

In questo laboratorio faremo ampio uso del tool *nslookup*, che è disponibile nella maggior parte delle piattaforme Linux/Unix e Microsoft. Per eseguire *nslookup* su Linux/Unix è sufficiente digitare *nslookup* dalla riga di comando. Per eseguirlo da Windows, aprite il prompt dei comandi e digitate *nslookup*.

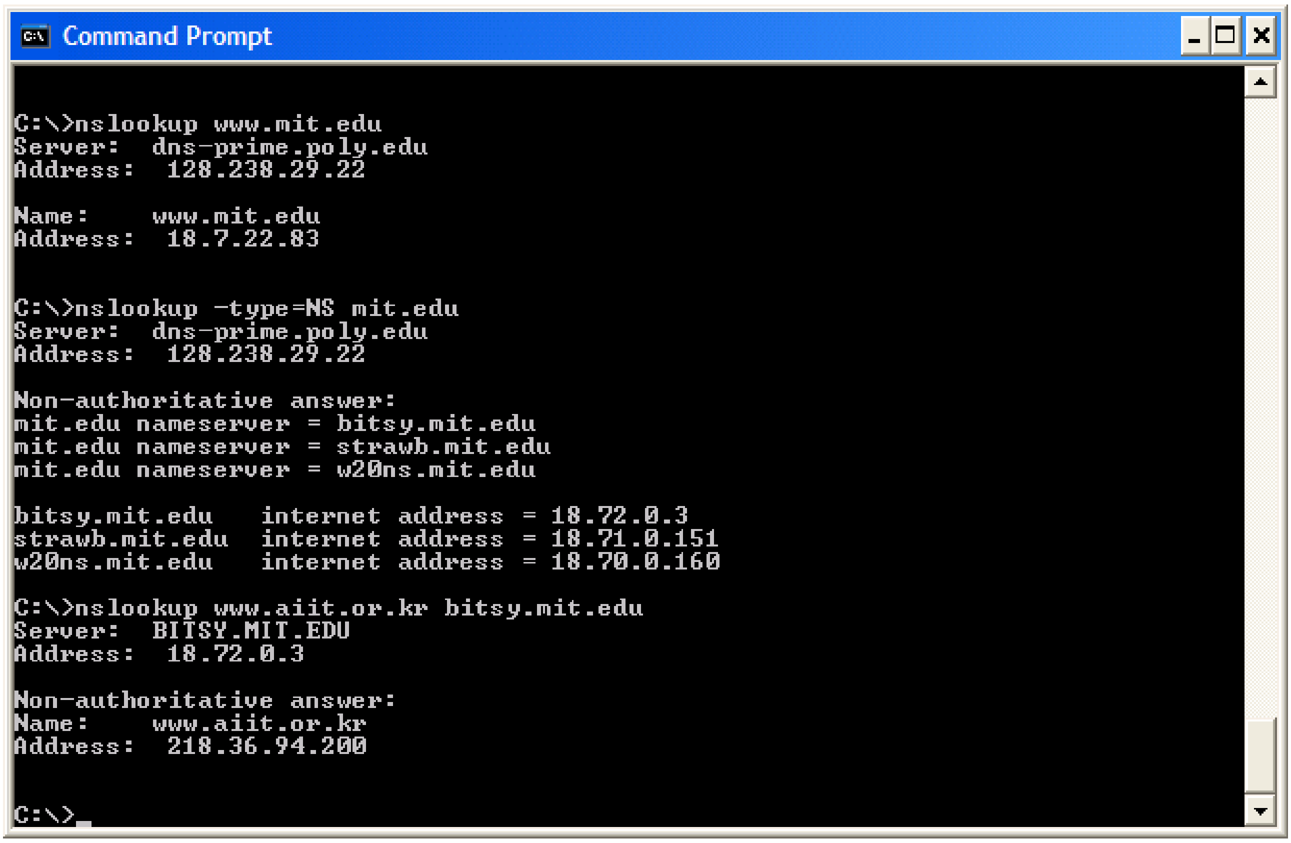
Nella sua forma più semplice, *nslookup* consente di interrogare un qualunque server DNS. Il server interrogato può essere un server radice, un server di dominio top-level, un server di competenza o un server DNS intermedio (controllare il libro di testo per la definizione di questi termini). Più in dettaglio, *nslookup* invia una query DNS al server DNS specificato, riceve una risposta dal server e visualizza il risultato.

Lo screenshot qui sotto mostra il risultato di tre comandi *nslookup* indipendenti (visualizzati all'interno di una finestra col prompt dei comandi). In questo esempio, il client si trova localizzato nel campus della Polytechnic University in Brooklyn, dove il server DNS locale è dns-prime.poly.edu. Quando si esegue *nslookup*, se non viene specificato alcun DNS, allora la query viene inviata al server di default.

Considerate il primo comando:

```
nslookup www.mit.edu
```

In parole, questo comando vuol dire "Per favore, mandami l'indirizzo IP dell'host www.mit.edu". Come mostrato nello screenshot, la risposta di questo comando contiene due informazioni differenti: (1) il nome e indirizzo IP del server DNS che fornisce la risposta; e (2) la risposta vera e propria, ovvero il nome dell'host e l'indirizzo IP di www.mit.edu. Sebbene la risposta sia venuta dal server DNS locale della Polytechnic , è del tutto possibile che questo DNS locale contatti iterativamente vari altri DNS per ottenere la risposta, come descritto nella sezione 2.5 del libro di



testo.

Ora considerate il secondo comando:

```
nslookup –type=NS mit.edu
```

In questo esempio, abbiamo fornito l'opzione “-type=NS” e il dominio “mit.edu”. Questo istruisce *nslookup* a mandare una interrogazione per record di tipo NS verso il server DNS locale. A parole, la query dice “Per favore, mandami i nomi dei server DNS di competenza per il dominio mit.edu.”. (Se l'oèzione -type non fosse usata, *nslookup* si comporterebbe normalmente, richiendo un record di tipo A; vedete Sezione 2.5.3 nel libro di testo.) La risposta, visualizzata nello screenshot di sopra, indica il server DNS che sta fornendo la risposta (che è il server DNS locale di default) assieme a tre nameserver del MIT. Ognuno di questi server è di competenza (autoritativo) per gli host del campus del MIT. Tuttavia, *nslookup* indica anche che questa risposta è “non-authoritative”, che vuol dire che è venuta dalla cache di qualche server piuttosto che dai server DNS del MIT. Infine, la risposta include anche l'indirizzo IP dei DNS autoritativi del MIT (Sebbene la query di tipo NS generata da *nslookup* non abbia richiesto esplicitamente gli indirizzi IP, il server DNS locale li ha restituiti “gratis”, e *nslookup* ha visualizzato il risultato.)

Infine, consideriamo il terzo comando:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

In questo esempio, abbiamo indicato che vogliamo mandare la query al server DNS bitsy.mit.edu, piuttosto che al server DNS di default (che, ricordiamo, si tratta di dns-prime.poly.edu). Così, la transazione costituita dalla query e relativa risposta ha luogo direttamente tra il nostro host richiedente e il server bitsy.mit.edu. In questo esempio, bitsy.mit.edu fornisce l'indirizzo IP dell'host www.aiit.or.kr, che è un web server dell'Advanced Institute of Information Technology (in Korea).

Ora che abbiamo visto qualche esempio illustrativo, vi starete probabilmente chiedendo quale sia la sintassi generale del comando *nslookup*. La sintassi è

```
nslookup -opzione1 -opzione2 host-da-cercare server-dns
```

In generale, *nslookup* può essere eseguito con zero, una, due o più opzioni. E, come abbiamo visto

negli esempi, il server-dns è anch'esso opzionale; se non è fornito, la query è inviata al server DNS locale di default.

Attenzione. In aula informatica non è possibile interrogare un server DNS a scelta. I firewall presenti nella rete consentono solo di interrogare il server DNS locale.

Ora che abbiamo fornito una panoramica di *nslookup*, è giunta l'ora di metterlo alla prova voi stessi. Fate quanto segue (e scrivete i risultati):

1. Eseguite nslookup per ottenere l'indirizzo IP di un server web in Asia
2. Eseguite nslookup per determinare i server DNS autoritativi di una università in Italia (diversa dalla Università di Chieti-Pescara).
3. Eseguite nslookup per determinare i server SMTP di Gmail
4. Eseguite nslookup per determinare il nome di host canonico di fad.unich.it
5. Solo se non siete in aula informatica, eseguite nslookup in modo tale che uno dei server ottenuti al punto 2 venga interrogato per ottenere i mail server di Gmail.

Ipconfig/ifconfig

ipconfig (per Windows) e *ifconfig* (per Linux/Unix) sono piccoli tool ma molto utili, specialmente quando si tratta di effettuare il debugging di connessioni di rete problematiche. *ipconfig* può essere usato per mostrare la configurazione TCP/IP corrente, incluso il vostro indirizzo, i server DNS, le interfacce di rete, e così via.

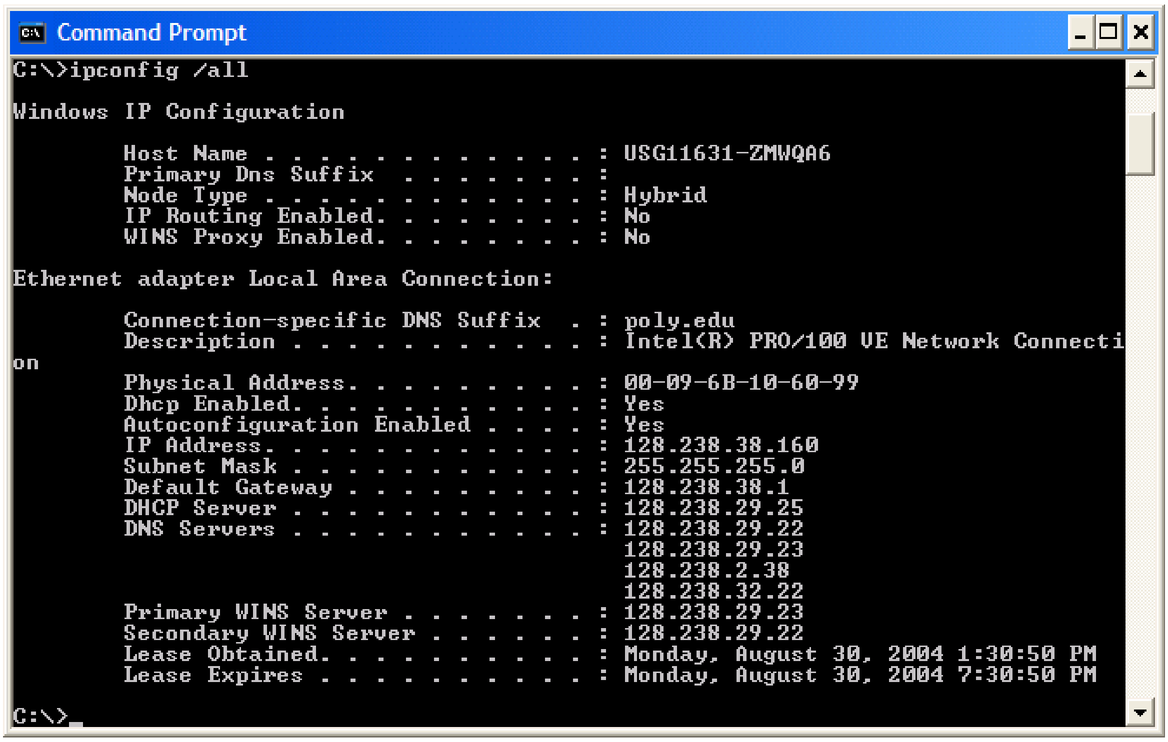
Per esempio, se volete vedere tutte le informazioni sul vostro host, digitate

```
ipconfig \all
```

nel prompt dei comandi, come mostrato nel seguente screenshot. Su sistemi Unix/Linux, il comando

```
ifconfig
```

genera un output analogo, sebbene presentato in maniera diversa.



```
Command Prompt
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : USG11631-ZMWQA6
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : poly.edu
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network Connecti
on
        Physical Address. . . . . . . . . : 00-09-6B-10-60-99
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 128.238.38.160
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 128.238.38.1
        DHCP Server . . . . . . . . . . . : 128.238.29.25
        DNS Servers . . . . . . . . . . . : 128.238.29.22
                                            128.238.29.23
                                            128.238.2.38
                                            128.238.32.22
        Primary WINS Server . . . . . . . : 128.238.29.23
        Secondary WINS Server . . . . . . : 128.238.29.22
        Lease Obtained. . . . . . . . . . : Monday, August 30, 2004 1:30:50 PM
        Lease Expires . . . . . . . . . . : Monday, August 30, 2004 7:30:50 PM

C:\>
```

ipconfig è anche molto utile per manipolare le informazioni sul DNS memorizzate nel vostro host. Nella Sezione 2.5 avete imparato che un host può mantenere i record DNS ottenuti di recente in una cache, Per vedere i record contenuti nella cache, basta dare il comando

```
ipconfig /displaydns
```

Ogni record contiene anche il TTL (Time to Live) rimanente in secondi. Per cancellare la cache, dare il comando:

```
ipconfig /flushdns
```

Linux/Unix non usa di default una cache DNS, sebbene sia possibile installare un software apposito chiama *nscd* (Name Server Cache Daemon). Pertanto, *ifconfig* non ha alcuna funzione relativa al DNS. Per visualizzare i server DNS locali, su Linux si può usare il comando

```
cat /etc/resolv.conf
```

Tracciare il protocollo DNS con Wireshark

Ora che abbiamo familiarizzato con *nslookup* e *ifconfig*/*ipconfig*, siamo pronti a lanciarci in qualche esercitazione più seria. Dapprima cattureremo i pacchetti DNS che sono generati dalla navigazione web ordinaria.

- Per Windows, usate *ipconfig* per svuotare la cache DNS. Per Linux, uscite da Firefox e rientrate (Firefox mantiene una sua cache locale delle risposte del DNS)
- Aprite il vostro browser e svuotate la cache (consultate l'esercitazione precedente per le istruzioni su come fare).
- Aprite Wireshark e immettete “dns or http” nel filtro. In questo modo verranno visualizzati solo i pacchetti relativi ai protocolli DNS e HTTP.
- Iniziare la cattura dei pacchetti con Wireshark.
- Col vostro browser, visitate la pagina web http://lupin.
- Interrompete la cattura dei pacchetti.

Se non siete in grado di eseguire Wireshark da un computer connesso direttamente a Internet, potete scaricare una traccia di pacchetti che è stata creata seguendo i passi di cui sopra, da uno dei computer degli autori[1].

Rispondete alle seguenti domande:

4. Localizzare le query DNS e i messaggi di risposta. Sono inviati sopra UDP o TCP?
5. Qual è la porta di destinazione per le query DNS? Qual'è la porta sorgente per i messaggi DNS di risposta?
6. A quale indirizzo IP è stata mandata la query DNS. Usate *ipconfig* (o *cat /etc/resolv.conf*) per determinare l'indirizzo IP del vostro server DNS locale. I due indirizzi IP sono uguali?
7. Esaminate la query DNS. Di che “Type” di query si tratta? La query contiene delle “risposte”?
8. Esaminate la risposta DNS. Quanti “record di risposta” sono forniti ? Che cosa contiene ognuno di questi record?
9. Considerate la query HTTP inviata successivamente dal vostro host. L'indirizzo IP

1 Scaricare il file zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip ed estrarre il file dns-ethereal-trace-1. Le tracce nel file zip sono state raccolte da Wireshark da uno dei computer dell'autore, seguendo i passati indicati nella lezione. Una volta scaricata la traccia, potete caricarla dentro Wireshark usando il menù a discesa File, scegliendo Open e selezionando il file dns-ethereal-trace-1.

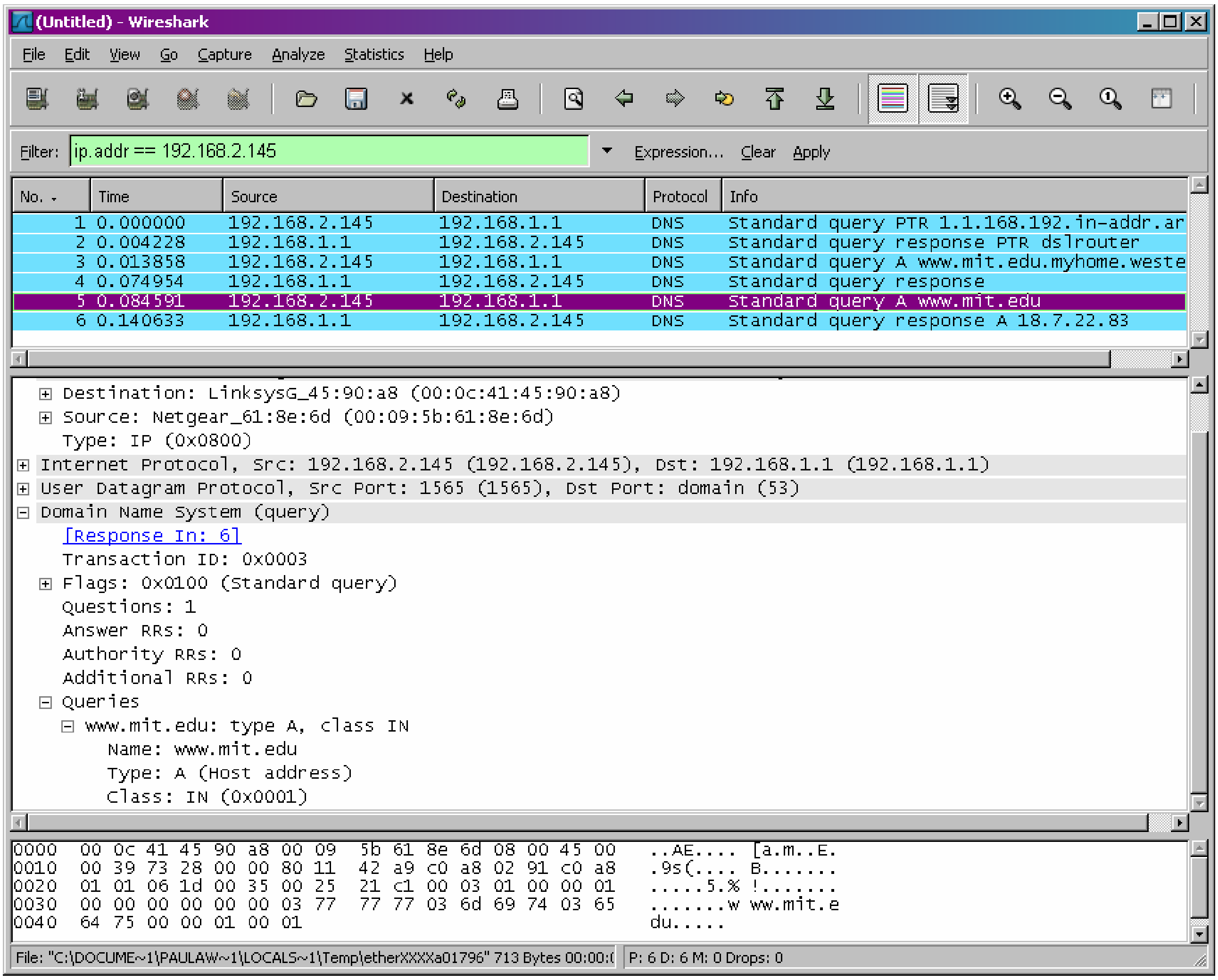
destinazione di questo pacchetto corrisponde a qualcuno degli indirizzi IP forniti nel messaggio di risposta DNS?

10. Questa pagina web contiene immagini. Prima di recuperare queste immagini, sono state inviate altre query DNS?

Ora giochiamo un po' con nslookup[2].

- Fate partire la cattura dei pacchetti.
- Fate un *nslookup* su www.mit.edu.
- Interrompete la cattura dei pacchetti.

Dovreste ottenere una traccia che assomiglia a questa:



Dallo screenshot di sopra possiamo vedere che in realtà *nslookup* ha inviato tre query DNS e ricevuto tre risposte. Per quanto riguarda questo esercizio, ignorate le prime due coppie richiesta/risposta (se ci sono), in quanto sono specifiche di nslookup e non vengono normalmente generate dalle applicazioni Internet standard. Focalizzatevi invece sull'ultima query e il relativo messaggio di risposta.

11. Qual'è la porta di destinazione per il messaggi DNS di richiesta. Qual'è la porta sorgente della risposta.

---

2 Se non siete in grado di eseguire Wireshark e catturare un traccia di esecuzione, usata la traccia dns-ethereal-trace-2 nel file zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.

12. A quale indirizzo IP è stata mandata la richiesta DNS. È questo l'indirizzo del vostro DNS locale?
13. Esaminate il messaggio di richiesta DNS nella finestra dei dettagli? Di che "Type" di query si tratta? Il messaggio contiene qualche "record di risposta"?
14. Esaminate il messaggio di risposta del server. Quanti "record di risposta" fornisce? Cosa contiene ognuno di essi?
15. Generare uno screenshot (premere il tasto Stampa)

Ora ripetete l'esperimento precedente, ma inviando il comando[3]:

```
nslookup –type=NS mit.edu
```

Rispondete alle seguenti domande:

16. A quale indirizzo IP è stata mandata la richiesta DNS. È questo l'indirizzo del vostro DNS locale?
17. Esaminate il messaggio di richiesta DNS nella finestra dei dettagli? Di che "Type" di query si tratta? Il messaggio contiene un qualche "record di risposta"?
18. Esaminate il messaggio di risposta del server. Quali nameserver del MIT sono contenuti nella risposta? Nel messaggio sono presenti anche gli indirizzi IP di questi nameserver ?
19. Generare uno screenshot (premere il tasto Stampa)

Se non vi trovate in aula informatica, ripetete l'esperimento precedente, ma inviando il comando[4]:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

Rispondete alle seguenti domande:

20. A quale indirizzo IP è stata mandata la richiesta DNS. È questo l'indirizzo del vostro DNS locale?
21. Esaminate il messaggio di richiesta DNS nella finestra dei dettagli? Di che "Type" di query si tratta? Il messaggio contiene qualche "record di risposta"?
22. Esaminate il messaggio di risposta del server. Quanti "record di risposta" fornisce? Cosa contiene ognuno di essi?
23. Generare uno screenshot (premere il tasto Stampa)

---

3 Se non siete in grado di eseguire Wireshark e catturare un traccia di esecuzione, usata la traccia dns-ethereal-trace-3 nel file zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.

4 Se non siete in grado di eseguire Wireshark e catturare un traccia di esecuzione, usata la traccia dns-ethereal-trace-4 nel file zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.